Report di Scansione Nessus

Data: 21/12/2023

Guglielmo Carratello

Dettagli della Scansione:

Strumento Utilizzato: Nessus

Data e Ora di Inizio: 16:00

Data e Ora di Fine: 16:30

Durata Totale della Scansione: 30 min

La sezione dei dettagli della scansione fornisce un contesto chiave, inclusi i tempi di inizio e fine, e la durata totale della scansione. Queste informazioni sono cruciali per valutare l'efficacia della scansione e pianificare eventuali azioni correttive.

Riepilogo Scansione:

La scansione è stata condotta per identificare vulnerabilità potenziali nel sistema Metasploitable2. I risultati di Nessus forniscono una panoramica delle possibili minacce e delle aree che richiedono attenzione prioritaria. Il riepilogo della scansione offre una visione generale degli obiettivi della scansione e del contesto in cui sono stati identificati i problemi di sicurezza.

Questa sezione prepara il terreno per una comprensione più approfondita dei risultati.

Vulnerabilità Rilevate:

Categoria: Critica

Sono state trovate 7 vulnerabilità di tipo critica

CRITICAL	10.0 *		NFS Exported Share Information Disclosure	RPC	1		
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1		
CRITICAL	10.0 *		VNC Server 'password' Password	Gain a shell remotely	1		
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	2		
CRITICAL	9.8		Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1		
CRITICAL	9.8		Bind Shell Backdoor Detection	Backdoors	1		
CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3		

Categoria: High

Sono state trovate 2 vulnerabilità di tipo High

HIGH	7.5		NFS Shares World Readable	RPC	1	
HIGH	7.5		Samba Badlock Vulnerability	General	1	

Categoria: Medium

Sono state trovate 10 vulnerabilità di tipo Medium

MIXED	...	...	SSL (Multiple Issues)	General	28	
MIXED	...	...	ISC Bind (Multiple Issues)	DNS	5	
MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	2	
MEDIUM	5.9		SSL Anonymous Cipher Suites Supported	Service detection	1	
MEDIUM	5.9		SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1	
MEDIUM	5.3		HTTP TRACE / TRACK Methods Allowed	Web Servers	1	
MIXED	...	...	SSH (Multiple Issues)	Misc.	6	
MIXED	...	...	SMB (Multiple Issues)	Misc.	2	
MIXED	...	...	TLS (Multiple Issues)	Misc.	2	
MIXED	...	...	TLS (Multiple Issues)	SMTP problems	2	

Categoria: Low

Sono state trovate 1 vulnerabilità di tipo Low

LOW	2.6 *		X Server Detection	Service detection	1	

Categoria: Info

Sono state trovate 123 info di possibili vulnerabilità

INFO	...	...	SMB (Multiple Issues)	Windows	7	
INFO	...	...	TLS (Multiple Issues)	General	4	
INFO	...	...	VNC (Multiple Issues)	Service detection	3	
INFO	...	...	Apache HTTP Server (Multiple Issues)	Web Servers	2	
INFO	...	...	FTP (Multiple Issues)	Service detection	2	
INFO	...	...	HTTP (Multiple Issues)	Web Servers	2	
INFO	...	...	PHP (Multiple Issues)	Web Servers	2	
INFO	...	...	RPC (Multiple Issues)	RPC	2	
INFO	...	...	SSH (Multiple Issues)	General	2	
INFO	...	...	SSH (Multiple Issues)	Service detection	2	
INFO			Nessus SYN scanner	Port scanners	25	
INFO			RPC Services Enumeration	Service detection	10	
INFO			Service Detection	Service detection	7	
INFO			Unknown Service Detection: Banner Retrieval	Service detection	4	
INFO			DNS Server Detection	DNS	2	
INFO			OpenSSL Detection	Service detection	2	
INFO			RMI Registry Detection	Service detection	2	

Questa sezione fornisce una panoramica dettagliata delle vulnerabilità identificate, inclusi dettagli sulla loro gravità e suggerimenti per la risoluzione. Ciascuna vulnerabilità dovrebbe essere valutata in base alla sua importanza per determinare le priorità di intervento.

Raccomandazioni:

Sulla base dei risultati della scansione, si consiglia di adottare le seguenti misure correttive:

Action	Vulns ▾	Hosts
ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS: Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.	3	1
Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.	0	1

Conclusione:

La scansione ha rivelato diverse vulnerabilità che richiedono un'attenzione immediata per garantire la sicurezza del sistema. Si raccomanda di implementare tempestivamente le soluzioni proposte per mitigare i rischi identificati.